What is Exploit?

Computer exploits or exploits are an attack taking advantage of a specific vulnerability on the system to help attackers infiltrate the computer.

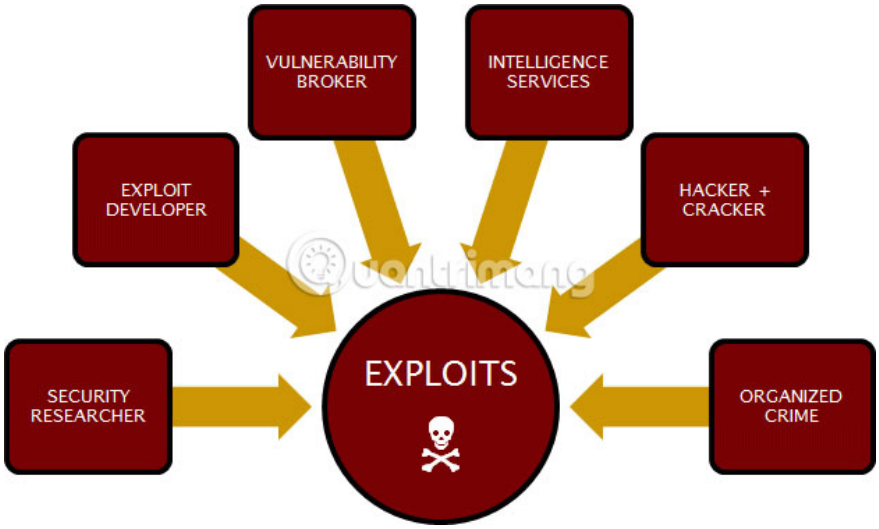
Computer exploits or exploits are an attack that takes advantage of a specific vulnerability on the system to help attackers infiltrate the computer. The term exploit refers to the successful implementation of such an attack.

The vulnerability attack exploits vulnerabilities in operating systems, applications, or any other software code, including software or application library plug-ins. Owners of these code sections often give a fix or patch to fix the problem. System or application users who are responsible for updating the patch, can often be downloaded from the software developer website or downloaded by the operating system or automated application. Failure to install a patch for a certain problem will cause the user to become a victim of computer exploits and potentially compromise security.

Find out about Computer exploit

1. Computer exploits
2. How does the exploit work?
3. Famous vulnerability exploits

Computer exploits



Security exploits appear in many different forms and sizes, some of which are frequently used. Some of the most popular web-based security vulnerabilities include SQL injection, cross-site scripting and cross-site attacks for forgery (attack techniques that use user authentication for another website). , as well as abuse of broken authentication code or incorrect security configuration.

Computer exploits can be categorized in different ways, depending on how they work and the type of attacks they can perform. The most common type of vulnerability exploitation is zero-day exploiting, taking advantage of the zero-day vulnerability. A zero-day vulnerability occurs when a software - usually an application or operating system - contains an important security vulnerability that the provider does not know. The flaw is only known when it is discovered that hackers are exploiting the vulnerability. That is why this term is called zero-day exploit. When an attack exploits such a vulnerability occurs, systems running the software will be vulnerable to attack, until the vendor releases a patch to fix vulnerabilities and users apply patches to the software. .

Computer exploits also have consequences like many other attacks, such as denial of service, remote code execution, privilege escalation (hacker hijacking the entire system), distributing malware, etc. . Computer exploit can also be divided by the type of exploited vulnerability, including buffer overflow, code injection or other types of input authentication vulnerabilities and side-channel attacks.

How does the exploit work?

Although exploiting vulnerabilities can happen in many different ways, the most common method is exploiting malicious websites. Victims may accidentally visit such a website or they may be tricked into clicking on a link to a malicious website in a phishing email or malicious ad.

Malicious sites used to exploit computer vulnerabilities can be equipped with exploitation packages, software tools, including malware that can be used as a basis for attacks. into different browser vulnerabilities, from a malicious website or from a hacked site. Such attacks often target software encoded in Java, the browser has not been updated to patch or browser plug-in. They are often used to deploy malware on a victim's computer.

Exploiting vulnerabilities automatically, such as by malicious websites, usually consists of two main components: Exploit code and shell code. Exploit code is software that tries to exploit a known vulnerability. Shell code is the payload of software designed to run when the target system is compromised. The shell code name comes from the fact that some of these payloads can open the shell to run commands against the target system.

Famous vulnerability exploits

In recent years, many attacks exploiting advanced vulnerabilities have been used to perform large-scale data violations and malware attacks. For example, in 2016, Yahoo announced that a hack occurred many years ago that caused data of 1 billion users to leak. Attackers have gained access to a user's email account because the password is protected by MD5, a weak and outdated hashing algorithm.

One of the most famous vulnerability exploits in recent years is EternalBlue, attacking a patched vulnerability in the Windows Server Message Block protocol. This attack was announced by the Shadow Brokers team and later used in the WannaCry and NotPetya ransomware attacks.

Most recently, Equachus Credit Reporting Company encountered a serious data breach attack, after attackers exploited the flaw in the Apache Struts framework, used in a public web application. company. A patch was released in early 2017, but Equachus did not update its web application until it discovered the attacker.